	Dokumentacja systemu SC PZU Życie	Wydanie: **1** Obowiązuje od:
Egz. nr	**Słownik pojęć**	

Opracował:	**Sprawdził:**	**Zatwierdził:**
Data: ..... *Podpis: .....*	*Data: .....* *Podpis*:	*Data: .....* *Podpis*: .....

Indeks

R

S

Ś

T

U

V

W

Z

Audyt – dokonanie niezależnego przeglądu i oceny działania systemu w celu przetestowania adekwatności środków nadzoru systemu, upewnienia się czy system działa zgodnie z ustaloną Polityką Certyfikacji i wynikającymi z niej procedurami operacyjnymi oraz w celu wykrycia przekłamań zabezpieczeń i zalecenia wskazanych zmian w środkach nadzorowania, polityce certyfikacji oraz procedurach.

Algorytm kryptograficzny - algorytm służący do szyfrowania i deszyfrowania informacji używanych w programach komunikacji sieciowej. Do podstawowych algorytmów kryptograficznych należą: DES, RSA, MD5, SHA, IDEA.

Bezpieczna ścieżka (*ang. trusted path*) – łącze zapewniające wymianę informacji związanych z uwierzytelnieniem użytkownika komputera, aplikacji lub innego urządzenia (np. identyfikacyjnej karty elektronicznej), zabezpieczone w sposób uniemożliwiający naruszenie integralności przesyłanych danych przez jakiekolwiek oprogramowanie.

Bean – klasa java posiadająca określone właściwości.

Centrum Certyfikacji - jednostka organizacyjna, będąca elementem składowym zaufanej trzeciej strony, obdarzonej zaufaniem w zakresie tworzenia i wydawania użytkownikom certyfikatów klucza publicznego

Certyfikat (certyfikat klucza publicznego) – wiadomość (patrz wiadomość), która zawiera co najmniej nazwę lub identyfikator urzędu certyfikacji, identyfikator subskrybenta, jego klucz publiczny, okres ważności certyfikatu, numer seryjny certyfikatu oraz jest podpisany przez urząd certyfikacji.

UWAGA: Certyfikat może znajdować się w jednym z trzech podstawowych stanów (patrz Stany klucza kryptograficznego): w oczekiwaniu na aktywność, aktywny i uśpiony.

Certyfikat ważny – certyfikat klucza publicznego jest ważny wtedy i tylko wtedy, gdy: (a) został wydany przez urząd certyfikacji, (b) został zaakceptowany przez podmiot wymieniony w tym certyfikacie oraz (c) nie jest unieważniony.

Certyfikat unieważniony – certyfikat, który został kiedyś umieszczony na liście certyfikatów unieważnionych, bez anulowania przyczyny unieważnienia (np. po odwieszeniu certyfikatu).

Certyfikat wzajemny (*ang. cross-certificate*) – jest to taki certyfikat klucza publicznego wydany urzędowi certyfikacji, w którym nazwy wystawcy i podmiotu tego certyfikatu są różne, klucz publiczny zawarty w certyfikacie może być używany jedynie do weryfikacji podpisów oraz wyraźnie jest zaznaczone, że certyfikat należy do urzędu certyfikacji.

Certyfikacja wzajemna (*ang. cross–certification*) – procedura wydawania certyfikatu przez urząd certyfikacji innemu urzędowi certyfikacji, który nie pozostaje z urzędem wydającym certyfikat w relacji bezpośredniego podporządkowania lub jest mu bezpośrednio podporządkowany. Zwykle certyfikat wzajemny wydawany jest w celu uproszczenia budowy i weryfikacji ścieżek certyfikatów, złożonych z certyfikatów wydawanych przez różne urzędu certyfikacji. Wydanie certyfikatów wzajemnych może być, ale nie jest to konieczne, realizowane na zasadzie wzajemności: tj. dwa urzędy certyfikacji wydają sobie nawzajem certyfikaty wzajemne.

Dane do audytu – chronologiczne zapisy aktywności w systemie pozwalające na zrekonstruowanie i analizowanie sekwencji zdarzeń oraz zmian, z którymi związane jest zarejestrowane zdarzenie.

Dane do przeglądu kontrolnego – patrz **dane do audytu**.

Dane uwierzytelniające - dane, które są przekazywane w celu ustalenia deklarowanej tożsamości podmiotu

Deskryptor – plik formatu xml opisujący właściwości beanów zdeplojowanych na serwerze wspierającym technologię J2EE

Deplojowanie – proces polegający na umieszczeniu oprogramowania na serwerze WebLogic. Może on następować w wyniku umieszczenia tego oprogramowania w katalogu <nazwa_domeny>/applications serwera WebLogic (w przypadku trybu pracy hot-deployment) lub też z wykorzystainem konsoli administracyjnej serwera WebLogic

- **wydeplojowanie** – analogicznie deplojowanie

- **oddeplojowanie** – proces polegający na usunięciu oprogramowania z serwera WebLogic. Może on następować w wyniku usunięcia tego oprogramowania z katalogu <nazwa_domeny>/applications serwera WebLogic (w przypadku trybu pracy hot-deployment) lub też z wykorzystaniem konsoli administracyjnej serwera WebLogic.

- **redeplojowanie** – proces polegający na ponownym wydeplojowaniu komponentu z wykorzystaniem konsoli administracyjnej serwera WebLogic. Aby przeprowadzić ten proces należy z konsoli administracyjnej wybrać polecenie „redeploy".

Dostęp – zdolność do korzystania z dowolnego zasobu systemu informacyjnego.

Dowód posiadania klucza prywatnego (POP, *ang. proof of possesion*) – informacja przekazana przez nadawcę do odbiorcy w takiej postaci, która umożliwia odbiorcy zweryfikowanie ważności powiązania istniejącego pomiędzy nadawcą a kluczem prywatnym, którym jest w stanie posłużyć się lub posługuje się; sposób przeprowadzenia dowodu jest uzależniony zwykle od rodzaju zastosowania pary kluczy; np. w przypadku kluczy podpisujących wystarczy, aby subskrybent przedłożył podpisany tekst (pozytywnie zakończona weryfikacja podpisu stanowi dowód posiadania klucza prywatnego), z kolei w przypadku kluczy szyfrujących subskrybent musi być w stanie odszyfrować informację zaszyfrowaną przy użyciu należącego do niego klucza publicznego. W SC PZU Życie weryfikacja powiązań pomiędzy parami kluczy stosowanych do podpisu i szyfrowania realizowana jest tylko przez urzędy rejestracji i urzędy certyfikacji.

Funkcjonalność SC PZU Życie – usługi certyfikacyjne udostępniane przez System Certyfikatów PZU Życie.

Główny Urząd Rejestracji (GUR) – urząd rejestracji, który oprócz standardowych czynności urzędu rejestracji akredytuje inne urzędy rejestracji.

Hot-deployment – tryb pracy serwera WebLogic, który pozwala na bieżąco obserwować zmiany następujące w domenie podczas zmiany oprogramowania (przeciwieństwem tego trybu pracy jest tryb produkcyjny)

Identyfikator obiektu (OID, *ang. Object Identifier*) – identyfikator alfanumeryczny/ numeryczny zarejestrowany zgodnie z normą ISO/IEC 9834 i wskazujący w sposób unikalny na określony obiekt lub klasę obiektów.

Infrastruktura klucza publicznego (PKI) – architektura, organizacja, techniki, zasady oraz procedury, które wspólnie wspomagają implementację i działanie kryptograficznych systemów klucza publicznego, opartych na certyfikatach. PKI składa się z powiązanych ze sobą elementów infrastruktury sprzętowej, programowej, baz danych, sieci, procedur bezpieczeństwa oraz zobowiązań prawnych, które dzięki współpracy realizują oraz udostępniają usługi certyfikacyjne, jak również inne związane z tymi elementami usługi (np. usługi znacznika czasu).

Integralność - zapewnia możliwość sprawdzenia, czy przesyłane dane nie zostały w żaden sposób zmodyfikowane podczas transmisji. Dzieje się tak dzięki dołączeniu do

wiadomości znacznika integralności wiadomości, czyli ciągu bitów obliczonego na podstawie wiadomości.

Karta kryptograficzna - jest osobistym urządzeniem służącym do realizacji podpisu elektronicznego, podnoszącym stopień bezpieczeństwa jego zastosowania.

Karta mikroprocesorowa - karta z wbudowanym układem mikroprocesorowym (chip). Może być stosowana jako bezpieczny nośnik informacji wrażliwej (np. kluczy prywatnych, certyfikatów). Specjalnym rodzajem karty mikroprocesorowej jest karta kryptograficzna czyli karta mikroprocesorowa z wbudowanym układem wspomagającym operacje kryptograficzne.

Keystore – magazyn certyfikatów specyficzny dla java, który przechowuje certyfikaty i klucze prywatne. Wszystkie zasoby są chronione za pomocą hasła.

Klucze infrastruktury – klucze kryptograficzne algorytmów szyfrowych stosowane przez SC PZU Życie do innych celów niż składanie lub weryfikacja podpisów pod wydawanymi certyfikatami i listami CRL, a w szczególności klucze stosowane: (a) do podpisywania i weryfikacji tokenów statusu certyfikatówe, (b) w protokołach uzgadniania lub dystrybucji kluczy zapewniających poufność danych, (c) dla zapewnienia, podczas transmisji lub przechowywania, poufności i integralności zgłoszeń certyfikacyjnych, kluczy użytkowników, rejestrów zdarzeń, (d) do weryfikacji dostępu do urządzeń lub aplikacji.

Klucz prywatny – klucz pary kluczy asymetrycznych podmiotu, który jest stosowany jedynie przez ten podmiot. W przypadku systemu podpisu asymetrycznego klucz prywatny określa przekształcenie podpisu. W przypadku systemu szyfrowania asymetrycznego klucz prywatny określa przekształcenie deszyfrujące.

UWAGI: (1) W kryptografii z kluczem publicznym klucz który jest przeznaczony do deszyfrowania lub podpisywania, do wyłącznego stosowania przez swego właściciela. (2) W systemie kryptograficznym z kluczem publicznym ten klucz z pary kluczy użytkownika, który jest znany jedynie przez tego użytkownika.

Klucz publiczny – klucz z pary kluczy asymetrycznych podmiotu, który może być uczyniony publicznym. W przypadku systemu podpisu asymetrycznego klucz publiczny określa przekształcenie weryfikujące. W przypadku systemu szyfrowania asymetrycznego klucz publiczny określa przekształcenie szyfrujące.

Klucz tajny – klucz wykorzystywany w symetrycznych technikach kryptograficznych i stosowany jedynie przez zbiór określonych subskrybentów.

UWAGA: Klucz tajny jest przeznaczony do stosowania przez bardzo mały zbiór korespondentów do szyfrowania i deszyfrowania danych.

Kodeks Postępowania Certyfikacyjnego SC PZU Życie – szczegółowy opis zasad i procedur udostępniania użytkownikom **usług certyfikacyjnych** świadczonych przez SC PZU Życie.

Kontrola dostępu – proces przekazywania dostępu do zasobów systemów informacyjnych tylko autoryzowanym użytkownikom, programom, procesom oraz innym systemom.

Kryptografia - dziedzina kryptologii zajmująca się projektowaniem algorytmów szyfrowania i deszyfrowania. Do zadań algorytmów należy zapewnienie tajności lub autentyczności komunikatów.

Lista certyfikatów unieważnionych (CRL, *ang. Certificate Revocation List*) – periodycznie (lub w trybie pilnym) wydawana lista podpisana cyfrowo przez urząd certyfikacji, umożliwiająca identyfikację certyfikatów które zostały zawieszone lub unieważnione przez upływem terminu ich ważności. Lista CRL zawiera nazwę wydawcy CRL, datę publikacji listy, datę następnej planowanej publikacji listy, numery seryjne zawieszonych lub unieważnionych certyfikatów oraz daty i przyczyny ich zawieszenia lub unieważnienia.

Magazyn certyfikatów - stały magazyn, w którym przechowywane są certyfikaty, odwołane certyfikaty i zaufane certyfikaty.

Mechanizm silnego uwierzytelnienia – procedura lub protokół uwierzytelniania za pomocą kryptograficznie uzyskanych **danych uwierzytelniających**.

Moduł kryptograficzny – zestaw składający się ze sprzętu, oprogramowania, mikrokodu lub ich określona kombinacja, realizujący operacje lub procesy kryptograficzne obejmujące szyfrowanie i deszyfrowanie wykonywane w obszarze kryptograficznym tego modułu.

Naruszenie (np. danych) – ujawnienie informacji nieuprawnionym osobom lub taka ingerencja naruszająca politykę bezpieczeństwa systemu, w wyniku której wystąpi nieuprawnione (zamierzone lub niezamierzone) ujawnienie, modyfikacja, zniszczenie lub udostępnienie dowolnego obiektu.

Nazwa wyróżniona (DN, *ang. distinguished name*) – zbiór atrybutów, tworzących nazwę wyróżnioną osoby prawnej, odróżniającą go od innych podmiotów tego samego typu; np. C=PL/S=mazowieckie/OU=PZU Życie SA, itp.

Niezaprzeczalność - zapobieganie odmowie poprzednich uzgodnień lub wykonania działań.

Obiekt – jednostka, do której dostęp jest kontrolowany, np. plik, program, obszar w pamięci głównej; gromadzone i utrzymywane dane osobowe (PN-2000:2002).

OCSP - protokół serwera weryfikacji statusu certyfikatów, pracującego w trybie on-line (ang. Online Certificate Status Protocol)

Okres aktywności certyfikatu – okres czasu pomiędzy początkową a końcową datą ważności certyfikatu lub pomiędzy datą początku ważności certyfikatu a datą jego unieważnienia lub zawieszenia.

Oświadczenie – własnoręcznie podpisana deklaracja Subskrybenta, stanowiąca podstawę udostępnienia mu przez SC PZU Życie funkcjonalności określonej w §2, pkt.2; oświadczenie to informuje Subskrybenta o jego zobowiązaniach oraz warunkach korzystania z funkcjonalności SC PZU Życie.

Parser – program, który dokonuje analizy danych wejściowych

PEM- standard bezpiecznej poczty elektronicznej. Ulepszony pod względem bezpieczeństwa schemat poczty elektronicznej, zwiększający prywatność korespondencji w sieci Internet. Wykorzystywany jest on zarówno do szyfrowania z jednym, jak i z parą kluczy (ang. Privacy Enhanced Mail).

PKCS # 12 - standard składni osobistej wymiany informacji specyfikujący przenośny format dla składowanych i przesyłanych kluczy prywatnych, certyfikatów i innych sekretów użytkownika.

PKCS # 7 - standard składni wiadomości szyfrowanej w sposób ogólny definiujący wiadomość kryptograficzną wzmocnioną przez podpis cyfrowy i szyfrowanie.

Podmiot certyfikatu – ten z użytkowników certyfikatu, którego dane umieszczone są w certyfikacie przez wystawcę tego certyfikatu.

Podpis cyfrowy – przekształcenie kryptograficzne jednostki danych, umożliwiające odbiorcy danych sprawdzenie pochodzenia i integralności jednostki danych oraz ochronę nadawcy i odbiorcy jednostki danych przed sfałszowaniem przez odbiorcę; asymetryczne podpisy cyfrowe mogą być generowane przez jeden podmiot przy zastosowaniu klucza prywatnego i algorytmu asymetrycznego, np. RSA.

Polityka certyfikacji – dokument w postaci zestawu reguł, które są ściśle przestrzegane przez urząd wydający certyfikaty w trakcie świadczenia przez niego usług certyfikacyjnych.

Polityka podpisu – szczegółowe rozwiązania, w tym techniczne i organizacyjne, wskazujące sposób, zakres oraz warunki potwierdzania oraz weryfikacji podpisu cyfrowego, których przestrzeganie umożliwia stwierdzenie ważności podpisu.

Posiadacz sekretu współdzielonego – autoryzowany posiadacz karty elektronicznej, na której przechowywany jest sekret współdzielony.

Poświadczenie - informacje, która użyte samodzielnie lub w powiązaniu z innymi informacjami stanowią dowód wystąpienia lub nie wystąpienia określonego zdarzenia lub działania.

Poświadczenie danych – wiarygodne potwierdzenie przez zaufaną stronę trzecią za pomocą podpisu cyfrowego statusu lub faktu istnienia przedłożonej do weryfikacji informacji, np. statusu certyfikatu lub podpisu cyfrowego.

Poświadczenie rejestracji danych - dane, zawierające poświadczenie stanowiące dowód zarejestrowania danych w elektronicznym archiwum.

Poufność - zagwarantowanie, że przesyłane lub przechowywane dane będą dostępne (możliwe do odczytania) jedynie dla uprawnionych osób, np.: odbiorcy wiadomości pocztowej. W szczególności chodzi o drukowanie, wyświetlanie i inne formy ujawniania, w tym ujawnianie istnienia jakiegoś obiektu.

PSE - osobiste bezpieczne środowisko (ang. personal security environment) jest to lokalny bezpieczny nośnik klucza prywatnego podmiotu, klucza publicznego (zwykle w postaci autocertyfikatu); w zależności od polityki bezpieczeństwa nośnik ten może mieć postać kryptograficznie zabezpieczonego pliku (np. zgodnie z PKCS#12) lub odporny na penetrację sprzętowy token (np. identyfikacyjna karta elektroniczna).

Procedura postępowania w sytuacji awaryjnej – procedura będąca alternatywą dla normalnej ścieżki realizacji procesu jeśli wystąpi sytuacja nadzwyczajna, lecz przewidywana.

Profil – skonkretyzowany opis struktury certyfikatu klucza publicznego, poświadczenia (w tym poświadczenia danych i rejestracji danych) lub tokenów w swoim zamierzeniu pozwalający na jednoznaczną interpretację ich zawartości.

Profil certyfikatu – skonkretyzowany opis struktury certyfikatu klucza publicznego, w swoim zamierzeniu pozwalający na jednoznaczną interpretację jego zawartości.

Protokół certyfikacji – logicznie uporządkowana wymiana informacji pomiędzy subskrybentem, urzędem rejestracji i urzędem certyfikacji w wyniku której następuje wydanie certyfikatu lub jego unieważnienie/zawieszenie.

Przejścia między stanami klucza – stan klucza kryptograficznego może ulec zmianie tylko w przypadku, gdy nastąpi jedno z przejść (zgodnie z normą ISO/IEC 11770-1):

generowanie – proces tworzenia klucza; generowanie klucza powinno być wykonywane zgodnie z ustalonymi zasadami generowania kluczy; proces może obejmować procedurę testową, służącą weryfikacji stosowania tych zasad,

aktywacja – powoduje, że klucz staje się uzyskuje ważność i może być stosowany w operacjach kryptograficznych,

deaktywacja – ogranicza użycie klucza; sytuacja taka może zdarzyć się na skutek upływu terminu ważności klucza lub unieważnienia klucza,

reaktywacja – umożliwia ponowne użycie klucza znajdującego się w stanie ustania aktywności do operacji kryptograficznych,

zniszczenie – powoduje zakończenie cyklu życia klucza; pod tym pojęciem rozumie się logiczne zniszczenie klucza, ale może także oznaczać zniszczenie fizyczne.

Publikowanie certyfikatów i list certyfikatów unieważnionych (CRL) (*ang. certificate and certificate revocation lists publication*) – Procedury dystrybucji utworzonych i unieważnionych certyfikatów. Dystrybucja certyfikatu obejmuje przesłanie go do subskrybenta oraz może obejmować jego publikację w repozytorium. Z kolei dystrybucja list certyfikatów unieważnionych oznacza umieszczenie ich w repozytorium, przesłanie do użytkowników końcowych lub przekazanie podmiotom które świadczą usługę weryfikacji statusu certyfikatu w trybie on-line. W obu przypadkach dystrybucja powinna być realizowana przy pomocy odpowiednich środków (np. LDAP, FTP, etc.).

Punkt zaufania – najbardziej zaufany urząd certyfikacji, któremu ufa subskrybent lub strona ufająca. Certyfikat tego urzędu jest pierwszym certyfikatem w każdej ścieżce certyfikacji, zbudowanej przez subskrybenta lub stronę ufająca. Wybór punktu zaufania jest zwykle narzucany przez politykę certyfikacji, według której funkcjonuje podmiot świadczący usługi certyfikacyjne.

Recertyfikacja (*ang. certificate update*) – Przed upływem okresu ważności certyfikatu urząd certyfikacji może odświeżyć go (zaktualizować), potwierdzając ważność tej samej pary kluczy na następny, zgodny z polityką certyfikacji, okres ważności.

Realm – security realm serwera WebLogic jest logiczną grupą zawierającą informacje o użytkownikach, grupach oraz ACL's. W grupie muszą znajdować się użytkownicy, którzy mają zamiar korzystać z zasobów chronionych na serwerze.

RSA - kryptograficzny algorytm asymetryczny (nazwa pochodzi od pierwszych liter jego twórców Rivesta, Shamira i Adlemana), w których jedno przekształcenie prywatne wystarcza zarówno do podpisywania jak i deszyfrowania wiadomości, zaś jedno przekształcenie publiczne wystarcza zarówno do weryfikacji jak i szyfrowania wiadomości.

Sekret unieważnienia certyfikatów – tajna informacja znana tylko subskrybentowi i urzędowi certyfikacji, wykorzystywana przez niego do uwierzytelniania żądań unieważniania certyfikatów w przypadku, gdy subskrybent nie posiada dostępu do prywatnego klucza podpisującego lub nie chce go użyć. Sekret unieważniania może być okresowo zmieniany.

Sekret współdzielony – część sekretu kryptograficznego, np. klucza, podzielonego pomiędzy n zaufanych użytkowników (dokładniej tokenów kryptograficznych typu, np. karty elektroniczne) w taki sposób, aby do jego zrekonstruowania potrzeba było m (m<n) części.

Skrzynka żądań – logiczny element systemu SC PZU Życie (np. bufor w postaci pliku przechowywanego na dysku twardym pod kontrolą systemu operacyjnego, do którego kierowane i z którego pobierane są tokeny zgłoszeń certyfikacyjnych.

Strona ufająca (*ang. relaying party*) – odbiorca, który otrzymał informację zawierającą certyfikat lub z nią powiązany oraz podpis cyfrowy weryfikowalny przy pomocy klucza publicznego umieszczonego w tym certyfikacie i znajdujący się w sytuacji, gdy na podstawie zaufania do certyfikatu musi podjąć decyzję o uznaniu lub odrzuceniu podpisu.

Sponsor subskrybenta – instytucja, która w imieniu subskrybenta finansuje usługi certyfikacyjne świadczone przez organ wydający certyfikaty. Sponsor jest właścicielem certyfikatu.

Stany klucza kryptograficznego (prywatnego, publicznego) - klucze kryptograficzne mogą znajdować się w jednym z trzech podstawowych stanów (zgodnie z normą ISO/IEC 11770-1):

w oczekiwaniu na aktywność (gotowy) – klucz został już wygenerowany, ale nie jest jeszcze dostępny do użytku,

aktywny – klucz może być używany w operacjach kryptograficznych (np. do realizacji podpisów cyfrowych),

uśpiony – w tym stanie klucz może być stosowany tylko i wyłącznie w operacjach weryfikacji podpisu cyfrowego lub deszyfrowania.

Subskrybent – jednostka (osoba fizyczna, osoba prawna, jednostka organizacyjna nie posiadająca osobowości prawnej, urządzenie, które jest pod opieką tych osób lub jednostki organizacyjnej), która; (1) jest podmiotem wymienionym lub zidentyfikowanym w certyfikacie wydanym tej jednostce, (2) posiada klucz prywatny, który odpowiada kluczowi publicznemu zawartemu w certyfikacie, oraz (3) sama nie wydaje certyfikatów innym stronom.

System informacyjny – całość infrastruktury, organizacja, personel oraz komponenty służące do gromadzenia, przetwarzania, przechowywania, przesyłania, prezentowania, rozgłaszania i zarządzanie informacją.

Szyfrowanie - kryptograficzne przekształcenie danych, którego wynikiem jest zaszyfrowany tekst (szyfrogram). Tekst taki dla osób trzecich stanowi jedynie przypadkowy ciąg znaków, na podstawie którego nie jest możliwe odtworzenie żadnej użytecznej informacji. Otrzymany w wyniku szyfrowania ciąg znaków nosi nazwę tekstu zaszyfrowanego (szyfrogramu).

Ścieżka certyfikacji – uporządkowany ciąg certyfikatów, prowadzący od certyfikatu **punktu zaufania**, wybranego przez weryfikującego, aż do weryfikowanego certyfikatu, utworzony w celu weryfikacji certyfikatu. Ścieżka certyfikacji spełnia następujące warunki:

- dla każdego certyfikatu Cert(x) należącego do ścieżki certyfikacji {Cert(1), Cert(2), ..., Cert(n-1)} podmiot certyfikatu Cert(x) jest wydawcą certyfikatu Cert(x+1),
- certyfikat Cert(1) jest wydany przez urząd certyfikacji (**punkt zaufania**), któremu ufa weryfikator,
- Cert(n) jest weryfikowanym certyfikatem.

Token – element danych stosowany w wymianach pomiędzy stronami zawierający informację, która została przekształcona z wykorzystaniem technik kryptograficznych. Token jest podpisany przez operatora urzędu rejestracji i może być wykorzystany do uwierzytelnienia jego nadawcy w trakcie kontaktów z urzędem certyfikacji.

Token niezaprzeczalności – zestaw istotnych danych, chronionych przy pomocy mechanizmów integralności oraz uwierzytelniania pochodzenia, zawierający poświadczenie.

Token zgłoszenia certyfikacyjnego – dane w postaci elektronicznej, zawierające zgłoszenie certyfikacyjne: (1) utworzone przez podmiot świadczący usługi certyfikacyjne, (2) potwierdzające tożsamość osoby i prawdziwość danych identyfikacyjnych zawartych w zgłoszeniu certyfikacyjnym, (3) opatrzone przez urząd rejestracji czasem jego przygotowania z minimalną dokładnością do jednej minuty, bez konieczności synchronizacji czasu oraz (4) opatrzone podpisem cyfrowym operatora urzędu rejestracji.

Token znacznika czasu – element danych, zawierający informację o czasie oraz dacie w sposób wiarygodny powiązany z dokumentem lub podpisem cyfrowym (zwykle z ich skrótami) i potwierdzony przez zaufany urząd znacznika czasu w sposób, który umożliwia wykrycie każdej modyfikacji.

Unieważnienie certyfikatu (ang. *certificates revocation*) - odwołanie ważności certyfikatu (i związanej z nim pary kluczy) i ostateczny koniec akceptowalnego stosowania certyfikatu w operacjach kryptograficznych (niezależnie od statusu tej operacji) począwszy od określonego momentu czasu; unieważniony certyfikat umieszczany jest na liście certyfikatów unieważnionych (CRL).

Urząd certyfikacji – obdarzona zaufaniem instytucja (np. SC PZU Życie), będąca elementem składowym zaufanej trzeciej strony, zdolna do tworzenia, podpisywania i wydawania certyfikatów.

Urząd rejestracji – obdarzona zaufaniem osoba prawna lub komórka organizacyjna PZU Życie, działająca na podstawie upoważnienia urzędu certyfikacji, rejestrująca osoby fizyczne i potwierdzająca ich tożsamość. Urząd rejestracji nie generuje pary kluczy, które można by poddać później procesowi certyfikacji.

Usługi certyfikacyjne – wydawanie certyfikatów, ich unieważnianie lub zawieszanie, wystawianie tokenów znacznika czasu, tokenów niezaprzeczalności, poświadczanie danych i poświadczanie rejestracji danych.

Uwierzytelnienie – mechanizm zabezpieczeń, którego zadaniem jest zapewnienie wiarygodności przesyłanych danych, wiadomości lub nadawcy, albo mechanizmy weryfikowania autoryzacji osoby przed otrzymaniem przez nią określonych kategorii informacji.

Użytkownik (certyfikatu, *ang. end entity*) – uprawniony podmiot, posługujący się certyfikatem jako subskrybent lub strona ufająca, z wyłączeniem urzędu certyfikacji.

Weryfikacja statusu certyfikatów (*ang. validation of public key certificates*) – weryfikacja statusu certyfikatów umożliwia określenie czy certyfikat jest unieważniony, czy też nie. Tego typu problem może być rozwiązany przez sam zainteresowany podmiot w oparciu o listy CRL albo też przez wystawcę certyfikatu lub upoważnionego przez niego przedstawiciela na wyraźne zapytanie podmiotu skierowane do serwera OCSP.

Wiadomość CMP – struktura danych przesyłana w ramach **protokołu certyfikacji**, zawierająca podpisaną cyfrowo odpowiedź urzędu certyfikacji i zgodna z normą ISO/IEC 15945.

Wnioskodawca – określenie używane w stosunku do subskrybenta w okresie pomiędzy chwilą, gdy wystąpił z jakimkolwiek żądaniem (wnioskiem) do urzędu certyfikacji a momentem ukończenia procedury wydawania certyfikatu.

Wydawanie certyfikatów – te spośród usług urzędu certyfikacji, które obejmują usługę rejestracji subskrybentów lub usługę certyfikacji klucza publicznego lub usługę aktualizacji klucza oraz certyfikatu, i kończą się utworzeniem certyfikatu kwalifikowanego, a następnie powiadomieniem o tym fakcie podmiotu wymienionego w treści tego certyfikatu lub fizycznym dostarczeniem mu utworzonego certyfikatu.

Zaufana Trzecia Strona (TTP ang. *Trusted Third Party*) – instytucja lub jej przedstawiciel mający zaufanie podmiotu uwierzytelnionego i/lub podmiotu weryfikującego oraz innych podmiotów w zakresie działań związanych z zabezpieczeniem oraz z uwierzytelnianiem.

Zastosowanie certyfikatu – certyfikat klucza publicznego wydany w ramach tej samej polityki certyfikacji, którego przeznaczenie (użycie) jest dobrze zdefiniowane w treści samego certyfikatu

Zawieszenie certyfikatu (ang. *suspension*) – szczególna forma unieważnienia certyfikatu (i związanej z nim pary kluczy), którego wynikiem jest czasowy brak akceptacji certyfikatu w operacjach kryptograficznych (niezależnie od statusu tej operacji); zawieszony certyfikat umieszczany jest na liście certyfikatów unieważnionych (CRL).

Zgłoszenie certyfikacyjne – zbiór dokumentów i danych identyfikujących podmiot podlegający certyfikacji.